

Keep your wireless networks safe

Keep hackers off your network and keep your business data secure



Wireless networks are becoming more and more common. Sometimes called Wi-Fi or 802.11 (after the standards which define how it works), they allow computers to connect to one another without cables. Using radio technology similar to cordless phones, they make it incredibly easy to connect to company networks, email and the internet. Unfortunately, they also make it very easy for outsiders to do the same.

Freeloading and freebooting

Anyone within radio range can, in theory, listen in or transmit data on your network. Even if they are sitting in a van in your car park or having a cup of coffee in the bar opposite your building.

This can mean somebody mooching off your expensive broadband internet connection, or worse, hacking into your network for more sinister reasons. Freely available tools allow would-be hackers to 'sniff' for insecure networks. Their task is made easier because many people do nothing to secure their network.

You will be found

Security firm RSA surveyed wireless security in the City of London. Using a handheld scanner they walked the streets and counted open networks. The results are alarming. One in four networks were not secure. Failures included:

- Not using the built-in encryption, making it easy to eavesdrop
- Using the default configuration for equipment, making it easy to gain access
- Using network names that identify the organisation

Some networks failed on all three counts. Businesses in the city are clearly embracing the new technology - the number of access points had tripled in the last year - but some of them are leaving themselves wide open to unauthorised access.

You will be hacked

RSA also tried to see whether people would take advantage of an open wireless network by setting up two 'honey pots' - wireless networks designed to look like unsecured corporate systems but actually containing sophisticated tools to track intruders. It took two and a half hours, on average, for someone to attempt an unauthorised connection. While many of the connections were caused by passers by carrying wireless-enabled laptops and palmtops which tried to access any nearby network, a quarter of the connections were by repeat 'offenders' who returned regularly to access the 'free' system.

How to secure a wireless network

It's not difficult to lock down a network. However, the actual procedure varies from manufacturer to manufacturer. In my case, with three PCs and a wireless-enabled Pocket PC, it took a couple of hours. This included time to read the manual (something I hate doing). This is what you need to do:

- Use access points only rather than ad-hoc, peer-to-peer networks
- Don't broadcast the name of the network (known as the SSID)
- Change the default SSID to something more obscure. Don't use a name that identifies your organisation
- If possible and if your access point allows it, restrict wireless access to normal office hours
- Use MAC filtering. Each network card has a unique code called a MAC address. You can set access points to restrict access to certain, trusted MAC addresses

- Switch on and use the built-in encryption to prevent eavesdropping
- Restrict the ability of users (and network administrators) to set up 'quick and dirty' wireless networks, even temporarily. One rogue access point can undo all the good work you do on the others
- Make sure all your other security measures - passwords etc. - are in place so that you have a second line of defence against intruders

For more advanced assistance, call PC Pal today on 01603 766716

From <http://www.microsoft.com/uk/smallbusiness/starting/technology-in-business/security/keep-wireless-networks-safe.mspx>